CLAIMS

What is claimed is:

1. In a computer system that comprises items, the items being stored in a volume, the volume divided into at least one security zone, each item residing in a single security zone a method of determining a principal's security rights to at least a portion of an item comprising:

an act of accessing authentication information that indicates the identity of a principal has been verified;

an act of accessing security rules for a security zone of the volume representing a principal's rights to at least one item in the security zone, the security rules having at least element, principal, and right arguments, at least one of the security rules specifying at least a portion of an item through an element path and at least one principal; and

an act of identifying the rights of the verified principal to the at least a portion of the item based on the accessed security rules.

2. The method of claim 1, the security rule being a grant of access to the at least a portion of the item.

3. The method of claim 1 further comprising, an act of granting the principal rights specified in the security rule if the principal is specified in the security rule.

4. The method of claim 3, the security rule specifying a plurality of principals.

5. The method of claim 4, the security rule including a deny ACE wherein the deny ACE excludes at least one principal from the plurality of principals.

6. The method of claim 5, the act of granting the at least one excluded principal rights specified in the security rule being performed if any other security rule for the security zone specifies that the at least one excluded principal has the right specified in the security rule.

7. The method of claim 3, the rights specified in the security rule being at least one of read, write, or delete access and the act of granting comprising allowing access to at least one attribute of the at least a portion of an item.

8. The method of claim 3, the rights specified in the security rule being execute access and the act of granting comprising allowing access to at least one method of the at least a portion of an item.

9. The method of claim 1, further comprising:

an act of receiving a query, the query comprising a query element argument, the query element argument comprising at least one element;

an act of returning the at least one element if the at least one element is included in the at least a portion of an item.

10. The method of claim 9, the at least one element being a complex element comprising a plurality of attributes, the act of granting being performed on all attributes

of the plurality of attributes.

11. The method of claim 1, further comprising:

an act of receiving a query, the query comprising a query element argument, the query element argument comprising at least one element; and

an act of returning a not-found message if the at least one element is not included in the at least a portion of an item of at least one of the security rules.

12. The method of claim 1, comprising an act of querying an API to determine security rights of an item, wherein the API computes security rights based on security rules specifying the item.

13. The method of claim 1, the security rule being an item in the volume.

14. The method of claim 1, further comprising the act of receiving a token, the token comprising data useful for authenticating the principal.

15. The method of claim 14, wherein the act of accessing authentication information comprises caching the identity of the principal for use in subsequent authentications during the same session.

16. The method of claim 1, wherein the act of accessing authentication information comprises consulting a cache entry to verify the identity of the principal.

17. The method of claim 1, the security rule including a deny ACE that excludes at least one element from the at least a portion of a data item.

18. The method of claim 1, the security rule specifying all rights by not specifying any rights.

19. The method of claim 1, the security rule comprising an item type argument specifying an item type, the method further comprising:

an act of receiving one of a query or request, the query or request comprising a query element argument comprising at least one element; and

an act of granting being performed if the at least one element is of the item type.

20. The method of claim 1, the security rule comprising an item type argument specifying an item type the method, further comprising:

an act of receiving one of a query or request the query or request comprising a query element argument comprising at least one element; and

an act of returning a not found being performed if the at least one element is not of the item type.

21. The method of claim 1, wherein the element argument specifies at least a portion of an item through an element path.

22. The method of claim 1, wherein the principal argument specifies at least one principal.

23. The method of claim 8, further comprising an act of executing the at least one method to create a security rule for a security zone from among the at least one security zone.

24. In a computer system that includes items stored in at least one volume, the volume being divided into at least one non-overlapping zone, each item residing in a zone from among the at least one non-overlapping zone, each zone having one or more principals with administrative rights, a method of delegating administrative rights to other principals for first items included in a main zone included in the at least one non-overlapping zone, comprising:

an act of identifying the first items in the main zone;

an act of splitting the main zone into a first zone and a remaining main zone, the one or more main principals retaining administrative rights for the first zone and the remaining main zone, the first zone including the first items and the remaining main zone including that portion of items in the main zone not included in the first items; and

an act of specifying that one or more first principals also have administrative rights to the first items.

25. The method of claim 24, specifying the one or more first principals is performed by the one or more main principals;

26. The method of claim 24 further comprising the act of labeling the first items with a zone enumeration corresponding to the first zone.

27. The method of claim 24, the administrative rights being security rights.

28. The method of claim 24, the administrative rights being auditing rights.

29. The method of claim 24 further comprising the act of specifying security rules for the first zone after the act of splitting.

30. The method of claim 24 comprising the act of specifying security rules for the first zone by defaulting security rules that were from the main zone prior to the act of splitting.

31. A method for creating a zone from the first zone and the remaining main zone recited in claim 24 comprising an act of re-combining the first zone and the remaining main zone.

32. A method for creating a zone from the first zone recited in claim 24 and a subsequent remaining main zone, the subsequent remaining zone formed from splitting the remaining main zone, wherein the administrative principals of the subsequent remaining main zone are the administrative principals in the main zone, comprising an act of re-combining the first zone and the subsequent remaining main zone.

33. A computer program product for use in a computer system that comprises items, the items being stored in a volume, the volume divided into at least one security zone, each item residing in a single security zone, the computer program product for implementing a method of determining a principals security rights to at least a portion of an item the computer program product comprising one or more computer-readable media having stored thereon computer-executable instructions that, when executed by a processor, cause the computer system to perform the following:

access authentication information that indicates the identity of a principal has been verified;

access security rules for a security zone of the volume representing a principal's rights to at least one item in the security zone, the security rules having at least element, principal, and right arguments, at least one of the security rules specifying at least a portion of an item through an element path and at least one principal; and

identify the rights of the verified principal to the at least a portion of the item based on the accessed security rules.

34. A computer program product for use in a computer system that includes items stored in at least one volume, the volume being divided into at least one non-overlapping zone, each item residing in a zone from among the at least one non-overlapping zone, each zone having one or more principals with administrative rights, the computer program product for implementing a method of delegating administrative rights to other principals for first items included in a main zone included in the at least one non-overlapping zone, the computer program product comprising one or more computer-readable media having stored thereon computer-executable instructions that, when executed by a processor, cause the computer system to perform the following::

identify the first items in the main zone;

split the main zone into a first zone and a remaining main zone, the one or more main principals retaining administrative rights for the first zone and the remaining main zone, the first zone including the first items and the remaining main zone including that portion of items in the main zone not included in the first items; and

specify that one or more first principals also have administrative rights to the first items.

35. In a computer system that includes items stored in at least one volume, the volume being divided into at least one non-overlapping zone, each item residing in a zone from among the at least one non-overlapping zone, each zone having one or more principals with administrative rights, a method of delegating administrative rights to other principals for first items included in a main zone included in the at least one non-overlapping zone, comprising:

a step for forming a first zone with first items, the first zone being formed from the main zone, one or main principals having administrative rights to the first items; and

an act of specifying that one or more first principals also have administrative rights to the first items.